AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

State and District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Apple Model A1465 Laptop Serial Number C02NH48TG083

Case No. 16mr197

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the State and District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1029	Fraud and related activity in connection with access devices.
18 U.S.C. 1028	Fraud and related activity in connection with identity documents.

The application is based on these facts:

See attached Affadavit, Attachment A, and Attachment B, incorporated herein by reference

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Ryan Palmiter, HSI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 3-15-16

Judge's signature

City and state: Albuquerque, New Mexico

Kirtan Khalas United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE APPLICATION FOR AN ORDER AUTHORIZING THE SEARCH OF; Apple Model A1465 Laptop Serial Number C02NH48TG083	**Magistrate No.**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

1. I, Special Agent Ryan Palmiter, am currently employed with Immigration and Customs Enforcement, U.S. Department of Homeland Security, Homeland Security Investigations (HSI), in Albuquerque, New Mexico. I have been employed with HSI since February 18, 2011. Prior to employment with HSI, I was employed as an Immigration Enforcement Agent, with Immigration and Customs Enforcement in 2008. I am currently assigned to the General Crimes Investigations group in Albuquerque, where I conduct investigations including but not limited to violations related to Identity/Benefit Fraud and Identity Theft. I have conducted numerous investigations involving Identify Theft and Fraud as well as prepared and executed several search and seizure warrants.

LOCATION OF PLACE TO BE SEARCHED

2. This affidavit is submitted in conjunction with an application for authorization to forensically search:

   A) Silver Apple Model A1465 laptop with serial number C02NH48TG083.

3. This affidavit is based upon information I have gained from my investigation, my personal observations, training and experience, as well as upon information related to me by other individuals, including law enforcement officers. In making this affidavit, I am relying on information from my own personal observations and in part on information received from Officer Aguirre with the New Mexico State Police (NMSP).

   Your affiant believes there is probable cause and respectfully requests an order authorizing the search of the electronics described in paragraph 2 and further described in Attachment A.

4. Since this affidavit is being submitted for the limited purpose of securing a search and seizure warrant, I have not included each and every fact known to me concerning this investigation but have set forth only the facts that I believe are necessary to establish

KK

probable cause to believe that evidence relating to violations of 18 U.S. Code § 1029, Fraud and Related Activity in Connection with Access Devices and 18 U.S. Code § 1028, Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information, will be located within the items described in attachment A.

BACKGROUND

5. On March 3, 2016, at approximately 1000 hours, NMSP Officer Aguirre contacted the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) for assistance. NMSP Officer Aguirre requested assistance in order to further investigate what he believed to be suspicious items inside the Subject Vehicle. Officer Aguirre relayed to HSI Special Agents Palmiter and Allen that he initiated a traffic stop on the Subject Vehicle for a traffic violation of Following Too Closely. The traffic stop was conducted on Interstate 40 eastbound at approximately mile marker 140. Encountered in the vehicle were the driver, Daryl Sandoval and one passenger, Monica Acosta.

6. Officer Aguirre relayed to HSI Special Agents that he observed a rental agreement for the vehicle which listed Acosta as the renter and only authorized driver. Registration information indicated the Subject Vehicle was registered to EAN Holdings LLC doing business as Enterprise-Rent-A-Car. Officer Aguirre informed HSI Special Agents that Sandoval did not possess a valid driver's license, only an identification card, and was not listed as an authorized driver on the rental agreement.

7. Officer Aguirre told HSI Special Agents that Sandoval said he and Acosta were traveling from Nevada to Albuquerque to visit family. Officer Aguirre advised HSI Special Agents that he had asked for and received consent from the driver, Daryl Sandoval, to conduct a canine search on the vehicle. The canine alerted to the odor of the presence of narcotics within the vehicle. Officer Aguirre began a search of the vehicle for the narcotics. Officer Aguirre opened a compartment located behind the passenger seat and below the floorboard of the vehicle. (This is a factory storage compartment referred to by the manufacturer as a "stow and go"). Discovered in this compartment was a credit card embosser, a credit card encoder/decoder, two grocery style shopping bags containing numerous prepaid credit/debit cards both in their original packaging and out, a fingernail file/buffer, and nail polish remover.

8. Officer Aguirre told HSI Special Agents Palmiter and Allen that he asked Sandoval what the items were in the storage compartment. Sandoval referenced the area and stated that one of the items was a typewriter. Officer Aguirre confronted Sandoval with the fact that none of the items he observed in the storage compartment were typewriters. Sandoval replied that he believed Officer Aguirre already knew what the items were.

9. Through the open passenger side sliding van door HSI Special Agents Palmiter and Allen could see in plain view the items Officer Aguirre described; a credit/debit card embosser, a credit/debit card encoder/decoder, two bags with numerous prepaid cards both opened and unopened, as well as the fingernail buffer. Your Affiant knows through training and experience that these items are commonly used to deface, alter, and convert common

KK

access cards in order to produce replicas of legitimate credit and debit cards. Special Agents Palmiter and Allen asked Sandoval if he was willing to speak to them but he declined. Sandoval also declined permission for Special Agents Palmiter and Allen to search the van.

10. Officer Aguirre informed Sandoval that he was free to leave however, HSI was securing the vehicle in order to obtain a search warrant. Officer Aguirre issued Sandoval a citation for following too closely and he was transported to the closest location which was the Route 66 Casino, and was released. The subject vehicle was photographed on site, sealed, and towed to the HSI Albuquerque office. In addition the NMSP and HSI Special Agents escorted the Subject Vehicle to the HSI office.

11. Your Affiant believes the items observed in plain sight inside the Subject Vehicle indicate criminal activity as it relates to identify theft, access device fraud and/or credit card fraud. Recent law enforcement investigations have uncovered an emerging trend in the use of stored value cards (prepaid cards) to transport/smuggle illicit proceeds throughout the United States and abroad. Credit card companies, such as Visa and MasterCard, and banks that issue cards, commonly referred to as "card issuers," have developed common standards that enable credit cards to be readily used throughout the world

12. A stored-value card may consist of a credit card company such as Visa, MasterCard and American Express. A stored value card is a payment card with a monetary value stored on the card itself. A major difference between a stored value card and a regular credit or debit card is that debit and credit cards are usually issued in the name of individual account holders, while stored-value cards may be anonymous. A stored value cards offers different types of options. For example, a stored value card may be disposed of when the value is used, or the card value may be "reloaded" with additional funds. In addition, the term stored value card means the funds and or data are physically stored on the card. These cards can be purchased at most retail locations. Subjects involved in criminal activity are attracted to using stored value cards, because there is no credit check required to obtain a stored value card, and the purchaser is not required to maintain a bank account to fund stored value card transactions.

13. The stored value cards offered by retailers consist of various brands, some with a preset denomination. It is not until the customer pays for the predetermined amount that the funds are loaded onto the card using the magnetic stripe embedded in the card. At this point, the stored value card is now carrying a monetary value.

14. Persons engaged in criminal activity often use stored value cards rather than transporting currency due to a number of reasons. These include but are not limited to the ease of transportability, the anonymity of the stored value card and the ability to reload the value of the card. The purchase of stored value cards with illicit funds allows criminals to conduct a series of transactions to distance the funds from their criminal source.

15. Persons engaged in criminal activity involving stored value cards often use a "reader

writer encoder" machine which allows them to remove any existing information stored on the magnetic stripe and replace it with stolen/compromised information. This information can include the credit account number and "track data" from an unsuspecting victim. Track Data is described as the categories of information encoded on the magnetic stripe of a credit card. In addition, an encoder machine can also place a victim's bank account information on the magnetic stripe. This allows the criminal to use a stored value card to purchase high end merchandise easily sellable on the black market while draining the funds of an unsuspecting victim's bank account.

16. On March 7, 2016, a federal search and seizure warrant was issued for the Subject Vehicle by a United States Magistrate Judge. HSI Special Agents executed the search warrant on the same date and recovered multiple prepacked stored value cards, a credit card decoder/encoder terminal, a credit card embossing machine, a point of sales terminal, and several finger nail buffers. These items were found in the Subject Vehicle's Stow and Go compartment located behind the front passenger seat.

17. In addition, a credit card stamping machine was also found in the Stow and Go compartment. Attached to the machine was gold foil used to imprint/stamp numbers on black cards. The foil had what appeared to be credit card numbers imprinted upon it.

18. Also found during the search was a black Apple IPad mini with serial number F4KJTEQRF19K, a silver Apple IPad mini with serial number DLXLN705FLMN, a red and black Hewlett Packard laptop with serial number 5CD42627NS, and a silver Apple Model A1465 laptop with serial number C02NH48TG083. The IPads and Hewlett Packard laptop were found in a black backpack that was on the seat behind the driver. The Apple Model A1465 was found in a green back on the seat located behind the front passenger.

19. Your affiant knows through his training, knowledge, and experiences that computers and electronic media are used to receive and store stolen/compromised credit card information. Also a computer or item of similar capabilities is needed to operate the credit card decoder/encoder found during the search.

20. Your affiant has probable cause to believe that records, evidence, fruits and instrumentalities relating to violations of 18 U.S. Code § 1029, Fraud and Related Activity in Connection with Access Devices and 18 U.S. Code § 1028, Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information are held within black Apple IPad mini with serial number F4KJTEQRF19K, a silver Apple IPad mini with serial number DLXLN705FLMN, a Hewlett Packard laptop with serial number 5CD42627NS, and an Apple Model A1465 laptop with serial number C02NH48TG083.

21. Your Affiant has probable cause to believe that there is evidence of involved in or traceable to a violation(s) of 18 U.S. Code § 1029, Fraud and Related Activity in Connection with Access Devices and 18 U.S. Code § 1028, Fraud and Related Activity in

Connection with Identification Documents, Authentication Features, and Information and are subject to seizure and forfeiture pursuant to Title 18 United States Code § 981 (a) (1).

WHEREFORE, I respectfully request that a warrant be issued authorizing Homeland Security Investigations, with appropriate assistance from other law enforcement officers, to forensically review a Silver Apple Model A1465 laptop with serial number C02NH48TG083 described in Attachment A and therein search for, seize, and examine the items set forth above and in Attachment B.

IV. SEARCH AND SEIZURE

Your Affiant knows based upon training, experience, and information relayed by law enforcement officers and others involved in the forensic examination of computers that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips as described in Attachment B. Searches and seizures of computers and computer-related media requires agents to seize all computers and computer-related media described in Attachment B to be processed by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

A. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

B. Searching computer systems requires the use of precise scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

C. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises.

D. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or

KK

"keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

E. I am aware, based upon my experience and training, that it is technologically possible for persons to remotely control devices such as those listed in Attachment A. Such remote control can be affected through viruses, Trojan horses, and other forms of malicious software. When devices such as those listed in Attachment A are used in furtherance of access device fraud or identity theft, the presence or absence of such malicious software can be important evidence in determining who is responsible for the use of such devices. Likewise, the presence or absence of security software designed to detect malicious software can be important evidence pertaining to the state of mind of the users of the devices.

In order to search for data that is capable of being read or interpreted by a computer and computer-related media described in Attachment B, law enforcement personnel will need to search, seize, image, copy, and examine the items listed in Attachment A, believed to be evidence and/or an instrumentality of a violation of 18 U.S. Code § 1029 and 18 U.S. Code § 1028, subject to the procedures set forth above.

This affidavit was reviewed and approved by AUSA Jonathon Gerson.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge. FURTHER AFFIANT SAYETH NOT.

Ryan Palmiter, Special Agent
Homeland Security Investigations

Subscribed and sworn before me this 15th day of March, 2016.

Kirtan Khalsa United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

The PROPERTY described as;

A) Silver Apple Model A1465 laptop with serial number C02NH48TG083.

These items are currently in the possession of Homeland Security Investigations at 5441 Watson Drive SE Albuquerque, NM 87106.

KK

ATTACHMENT B

Items to be searched, seized and analyzed include all evidence, fruits and instrumentalities pertaining to violations of Title 18, United States Code § 1028A – Aggravated Identity Theft and Title 18, United States Code § 1029 – Access Device Fraud, and contained within the devices listed in attachment A.

Records and electronically stored documents that show the communications concerning identity theft and/or fraud/misuse of visas permits and other documents; as well as evidence of Title 18, United States Code § 1029 – Access Device Fraud

1. Computer hard drives, or other physical objects upon which computer data can be recorded that is called for by this warrant, or that might contain things otherwise called for by this warrant including:
   a. Evidence of who used, owned, or controlled the items described in Attachment A at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.
   b. Evidence of software that would allow others to control the items described in Attachment A, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.
   c. Evidence of the lack of such malicious software;
   d. Evidence of the attachment of other storage devices or similar containers for electronic evidence.
   e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the items described in Attachment A.
   f. Evidence of the times the items described in Attachment A was used.
   g. Passwords, encryption keys, and other access devices that may be necessary to access the items described in Attachment A.
   h. Contextual information necessary to understand the evidence described in this attachment.
   i. Records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

2. During the course of the search, photographs of the searched property may also be taken to record the condition thereof and/or the location of items therein.

KK